(/)

GARBAGE IN, GARBAGE OUT

FACE RECOGNITION ON FLAWED DATA

Clare Garvie

May 16, 2019

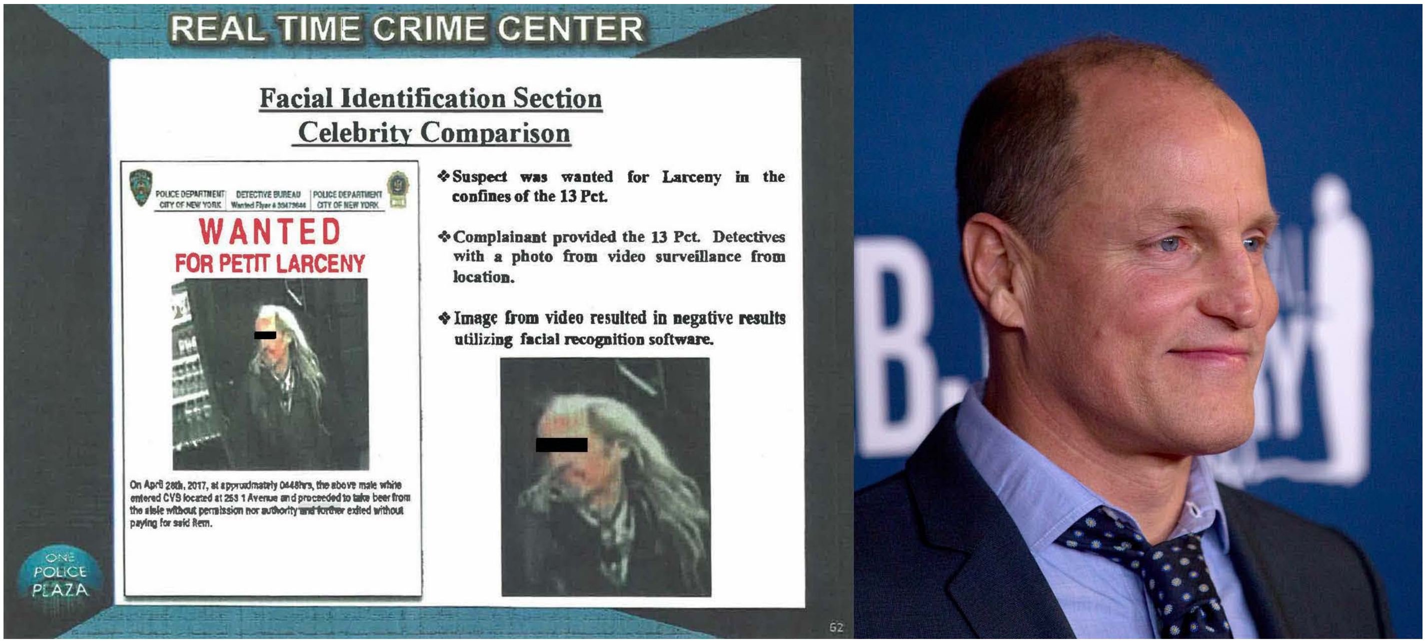
INTRODUCTION

On April 28, 2017, a suspect was caught on camera reportedly stealing beer from a CVS in New York City. The store surveillance camera that recorded the incident captured the suspect's face, but it was partially obscured and highly pixelated. When the investigating detectives submitted the photo to the New York Police Department's (NYPD) facial recognition system, it returned no useful matches.[1]

Rather than concluding that the suspect could not be identified using face recognition, however, the detectives got creative.

One detective from the Facial Identification Section (FIS), responsible for conducting face recognition searches for the NYPD, noted that the suspect looked like the actor Woody Harrelson, known for his performances in *Cheers*, *Natural Born Killers*, *True Detective*, and other television shows and movies. A Google image search for the actor predictably returned high-quality images, which detectives then submitted to the face recognition algorithm in place of the suspect's photo. In the resulting list of possible candidates, the detectives identified someone they believed was a match—not to Harrelson but to the suspect whose photo had produced no possible hits.[2]

This celebrity "match" was sent back to the investigating officers, and someone who was not Woody Harrelson was eventually arrested for petit larceny.



REAL TIME CRIME CENTER

Facial Identification Section
Celebrity Comparison

POLICE DEPARTMENT CITY OF NEW YORK | DETECTIVE BUREAU Wanted Flyer # 33473644 | POLICE DEPARTMENT CITY OF NEW YORK

WANTED
FOR PETIT LARCENY

On April 28th, 2017, at approximately 0448hrs, the above male white entered CVS located at 253 1 Avenue and proceeded to take beer from the aisle without permission nor authority ~~and further~~ exited without paying for said item.

- Suspect was wanted for Larceny in the confines of the 13 Pct.
- Complainant provided the 13 Pct. Detectives with a photo from video surveillance from location.
- Image from video resulted in negative results utilizing facial recognition software.

Figure 1: On the left: a slide from the NYPD FIS describing its "celebrity comparison" technique. On the right, a photo of Woody Harrelson. (Source: left, NYPD; right, Gabriel Cristóver Pérez/LBJ Presidential Library.)

There are no rules when it comes to what images police can submit to face recognition algorithms to generate investigative leads. As a consequence, agencies across the country can—and do—submit all manner of "probe photos," photos of unknown individuals submitted for search against a police or driver license database. These images may be low-quality surveillance camera stills, social media photos with filters, and scanned photo album pictures.[3] Records from police departments show they may also include computer-generated facial features, or composite or artist sketches.[4]

Or the probe photo may be a suspect's celebrity doppelgänger. Woody Harrelson is not the only celebrity to stand in for a suspect wanted by the NYPD. FIS has also used a photo of a New York Knicks player to search its face recognition database for a man wanted for assault in Brooklyn.[5]

The stakes are too high in criminal investigations to rely on unreliable—or wrong—inputs. It is one thing for a company to build a face recognition system designed to help individuals find their celebrity doppelgänger[6] or painting lookalike[7] for entertainment purposes. It's quite another to use these techniques to identify criminal suspects, who may be deprived of their liberty and ultimately prosecuted based on the match. Unfortunately, police departments' reliance on questionable probe photos appears all too common.

GARBAGE IN, GARBAGE OUT

"Pray, Mr. Babbage, if you put into the machine wrong figures, will the right answers come out?"

—Charles Babbage[8]

"Garbage in, garbage out" is a phrase used to express the idea that inputting low-quality or nonsensical data into a system will produce low-quality or nonsensical results. It doesn't matter how powerful or cleverly-designed a system is, it can only operate on the information it is provided—if data is missing, the system cannot operate on it. Any attempt to reconstruct or approximate missing data will necessarily be a "guess" as to what information that data contained.

Worse, if data is wrong—like a photo of someone other than the suspect—the system has no way to correct it. It has literally no information about the suspect, and can't make it up.

Photos that are pixelated, distorted, or of partial faces provide less data for a face recognition system to analyze than high-quality, passport-style photos, increasing room for error.[9]

Face recognition technology has improved immensely in the past two years alone, enabling rapid searches of larger databases and more reliable pairings in testing environments.[10] But it doesn't matter how good the machine is if it is still being fed the wrong figures—the wrong answers are still likely to come out.

1. COMPOSITE SKETCHES AS PROBE IMAGES

"Composite art is an unusual marriage of two unlikely disciplines: police investigative work and art .... It is essential to realize that a composite sketch is a drawing of a victim's or witness's perception of a perpetrator at the time he or she was observed. It is not meant to be an exact portrait of the suspect. Keep the two words 'likeness' and 'similarity' in mind at all times. This is the best a composite sketch can achieve."

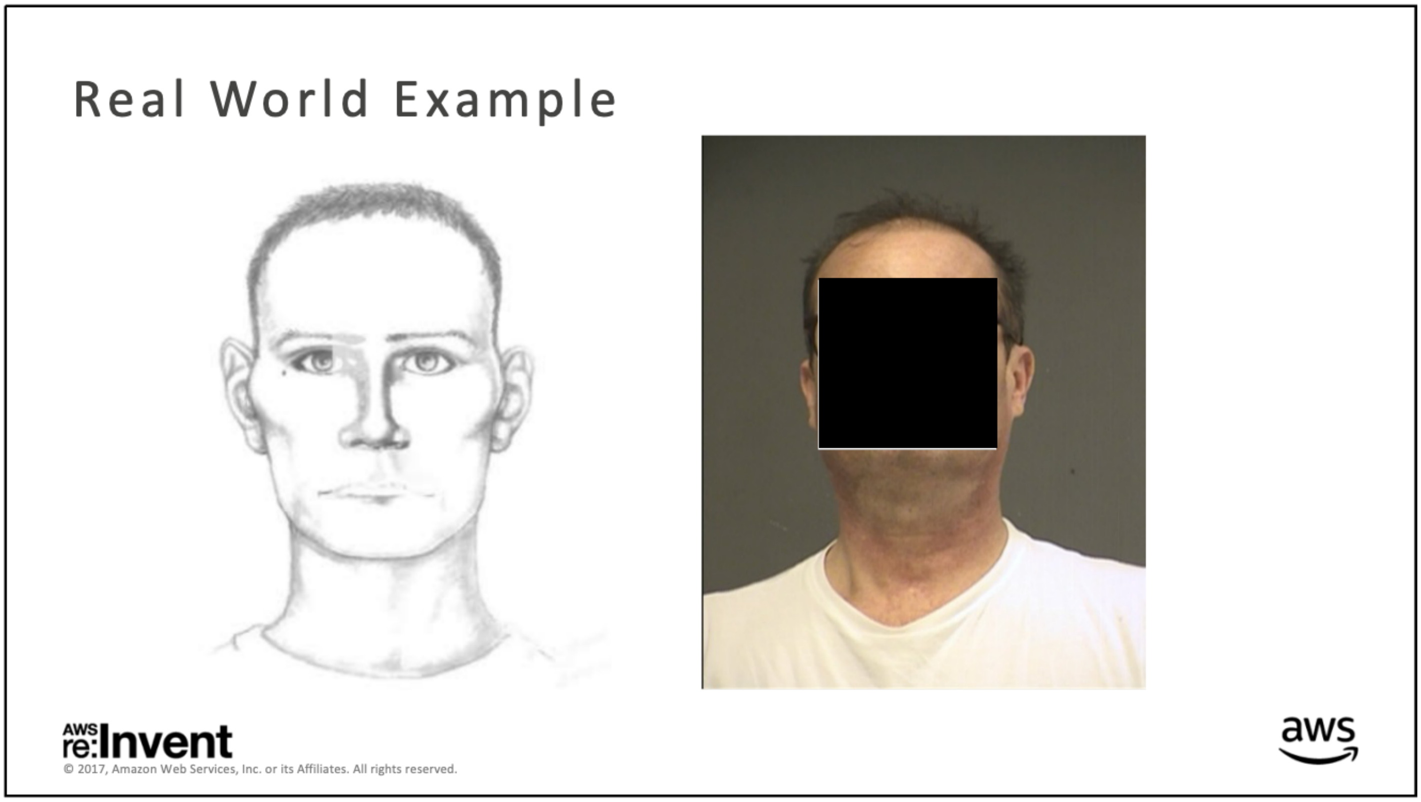
—*The Police Composite Sketch*[11]

In early 2018, Google rolled out "Art Selfie" — an app designed to match a user's photo to a famous painting lookalike using face recognition.[12] The result is an often-humorous photo pairing and an opportunity to learn more about art.

Less humorous is the fact that some police departments do the same thing when looking for criminal suspects, just in reverse—submitting art in an attempt to identify real people.

At least half a dozen police departments across the country permit, if not encourage, the use of face recognition searches on forensic sketches.

At least half a dozen police departments across the country permit, if not encourage, the use of face recognition searches on forensic sketches—hand drawn or computer generated composite faces based on descriptions that a witness has offered. In a brochure informing its officers about the acquisition of face recognition, the Maricopa County Sheriff's Office in Arizona states: "[T]he image can be from a variety of sources including police artist renderings," and that the technology "can be used effectively in suspect identifications using photographs, surveillance still and video, suspect sketches and even forensic busts."[13] A presentation about the face recognition system that the Washington County Sheriff's Department in Oregon operates includes a "Real World Example" of the technology being used to identify an artist's drawing of a face.[14]



Real World Example

[redacted]

AWS re:Invent

© 2017, Amazon Web Services, Inc. or its Affiliates. All rights reserved.

aws

Figure 2: Slide from an AWS presentation titled "Washington County Sheriff's Office Rekognition Case Study." (Source: Public records obtained by ACLU Oregon & Northern California.)

A face recognition Privacy Impact Assessment that a working group of 15 state and federal agencies authored in 2011 states that it should be permissible to use face recognition to "...identify suspects based upon artist's sketches."[15] Information about the Maryland Department of Public Safety and

Correctional Services, the Northern Virginia Regional Information System, and the Pinellas County Sheriff's Office in Florida suggest that sketches could be submitted to these agencies' face recognition systems as well.[16]

This practice is endorsed by some of the companies providing these face recognition systems to police departments. The example from the Washington County in Figure 2 is part of a case study that Amazon Web Services highlighted in a presentation about the capabilities of its face recognition software, Rekognition. Cognitec, one of the leading providers of face recognition algorithms to U.S. law enforcement, promotes the use of its software to "identify individuals in crime scene photos, video stills and sketches."[17] Vigilant Solutions markets tools specifically for "creating a proxy image from a sketch artist or artist rendering" to be submitted to its face recognition system.[18]

A. SCIENTIFIC REVIEW OF COMPOSITE IMAGE FACE RECOGNITION

Even the most detailed sketches make poor face recognition probe images. The Los Angeles County Sheriff’s Department face recognition user guide summarizes this well:

> "A photograph taken of a real person should be used. Composite drawing will have marginal success because they are rendered pictures and do not accurately detail precise features."[19]

Studies that have analyzed the performance of face recognition systems on composite sketches conclude the same. A 2011 Michigan State University study noted that "[c]ommercial face recognition systems are not designed to match forensic sketches against face photographs."[20] In 2013, researchers studying this question ran sketches against a face recognition database using a commercially-available algorithm from Cognitec—one of the companies that advertises this as a feature of its system. The algorithm was programmed to return a list of 200 possible matches searching a database of 10,000 images. For sketches, it retrieved the correct match between 4.1 and 6.7 percent of the time.[21] Put another way, in only about 1 of every 20 searches would the correct match show up in the top 200 possible matches that the algorithm produced.[22]

In 2014, the National Institute of Standards and Technology (NIST) found similarly poor results, concluding that "[s]ketch searches mostly fail."[23] The NYPD has separately concluded the same thing from their own experience. According to NYPD detective Tom Markiewicz, FIS has tried running face recognition on sketches in the past and found that "sketches do not work."[24] So did the Pinellas County Sheriff's Office, concluding that the practice "is doubtful on yielding successful results with the current [system]" —yet it still permits the practice nonetheless.[25]

B. FORENSIC SKETCHES AND MISIDENTIFICATION

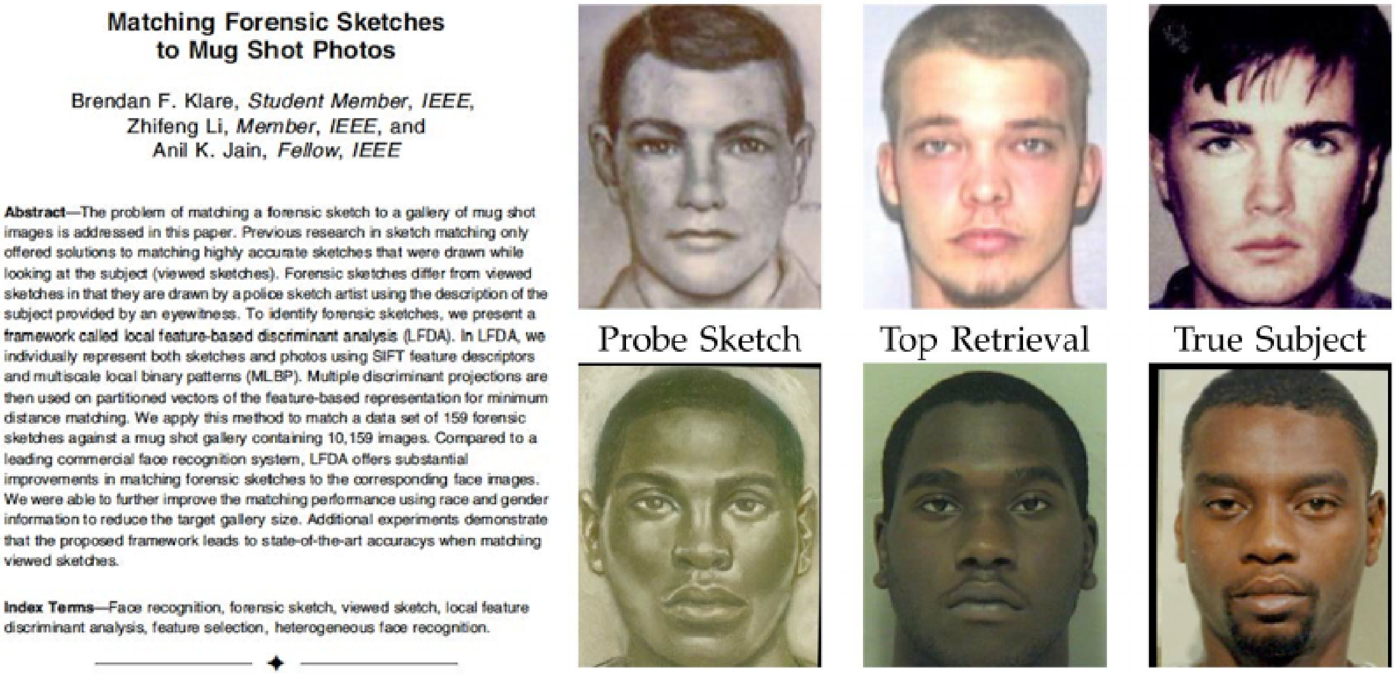
The most likely outcome of using a forensic sketch as a probe photo is that the system fails to find a match—even when the suspect is in the photo database available to law enforcement. With this outcome, the system produces no useful leads, and investigating officers must go back to the drawing board.

But this practice also introduces the possibility of misidentification. The process of generating a forensic sketch is inherently subjective. Sketches typically rely on:

a. An eyewitness's memory of what the subject looked like;

b. The eyewitness's ability to communicate the memory of the subject to a sketch artist;

c. The artist's ability to translate that description into an accurate drawing of the subject's face, someone whom the artist has never seen in person.[26]



Matching Forensic Sketches to Mug Shot Photos

Brendan F. Klare, *Student Member, IEEE*, Zhifeng Li, *Member, IEEE*, and Anil K. Jain, *Fellow, IEEE*

Abstract—The problem of matching a forensic sketch to a gallery of mug shot images is addressed in this paper. Previous research in sketch matching only offered solutions to matching highly accurate sketches that were drawn while looking at the subject (viewed sketches). Forensic sketches differ from viewed sketches in that they are drawn by a police sketch artist using the description of the subject provided by an eyewitness. To identify forensic sketches, we present a framework called local feature-based discriminant analysis (LFDA). In LFDA, we individually represent both sketches and photos using SIFT feature descriptors and multiscale local binary patterns (MLBP). Multiple discriminant projections are then used on partitioned vectors of the feature-based representation for minimum distance matching. We apply this method to match a data set of 159 forensic sketches against a mug shot gallery containing 10,159 images. Compared to a leading commercial face recognition system, LFDA offers substantial improvements in matching forensic sketches to the corresponding face images. We were able to further improve the matching performance using race and gender information to reduce the target gallery size. Additional experiments demonstrate that the proposed framework leads to state-of-the-art accuracys when matching viewed sketches.

Index Terms—Face recognition, forensic sketch, viewed sketch, local feature discriminant analysis, feature selection, heterogeneous face recognition.

Figure 3: Examples where an imposter, not the subject of the forensic sketch, is returned as the highest ranking face recognition match. (Source: Klare, Li, & Jain (2010), all rights reserved.)

Each of these steps introduces elements of subjective interpretation and room for error.[27] For example, an eyewitness may not remember the shape of the subject's jaw, yet the resulting sketch will necessarily include one. Or the witness may remember the suspect had "bug eyes," something the artist would need to interpret figuratively rather than literally.[28] As a consequence, the resulting sketch may actually look more like someone in the face recognition database other than the subject being searched for, as illustrated in Figure 3.

In this scenario, human review of the face recognition matches will not be able to remove the risk of error. When examining the face recognition results for a possible match, the analyst will have only the sketch to refer back to. The analyst will have no basis to evaluate whether the image accurately represents the subject being searched for. This compounds the risk that the face recognition search will lead to an investigation, if not an arrest, of the wrong person.

2. AN ART OR A SCIENCE? COMPUTER-GENERATED FACIAL FEATURES

A white paper titled "Facial Recognition: Art or Science?" published by the company Vigilant Solutions posits that face recognition systems—even without considering composite sketches—are "[p]art science and part art."[29] The "art" aspect is the process of modifying poor quality images before submitting them to a recognition algorithm to increase the likelihood that the system returns possible matches.[30]

Editing photos before submitting them for search is common practice, as suggested by responses to records requests and a review of the software packages that face recognition vendor companies offer. These documents also illustrate that the edits often go well beyond minor lighting adjustments and color correction, and often amount to fabricating completely new identity points not present in the original photo.

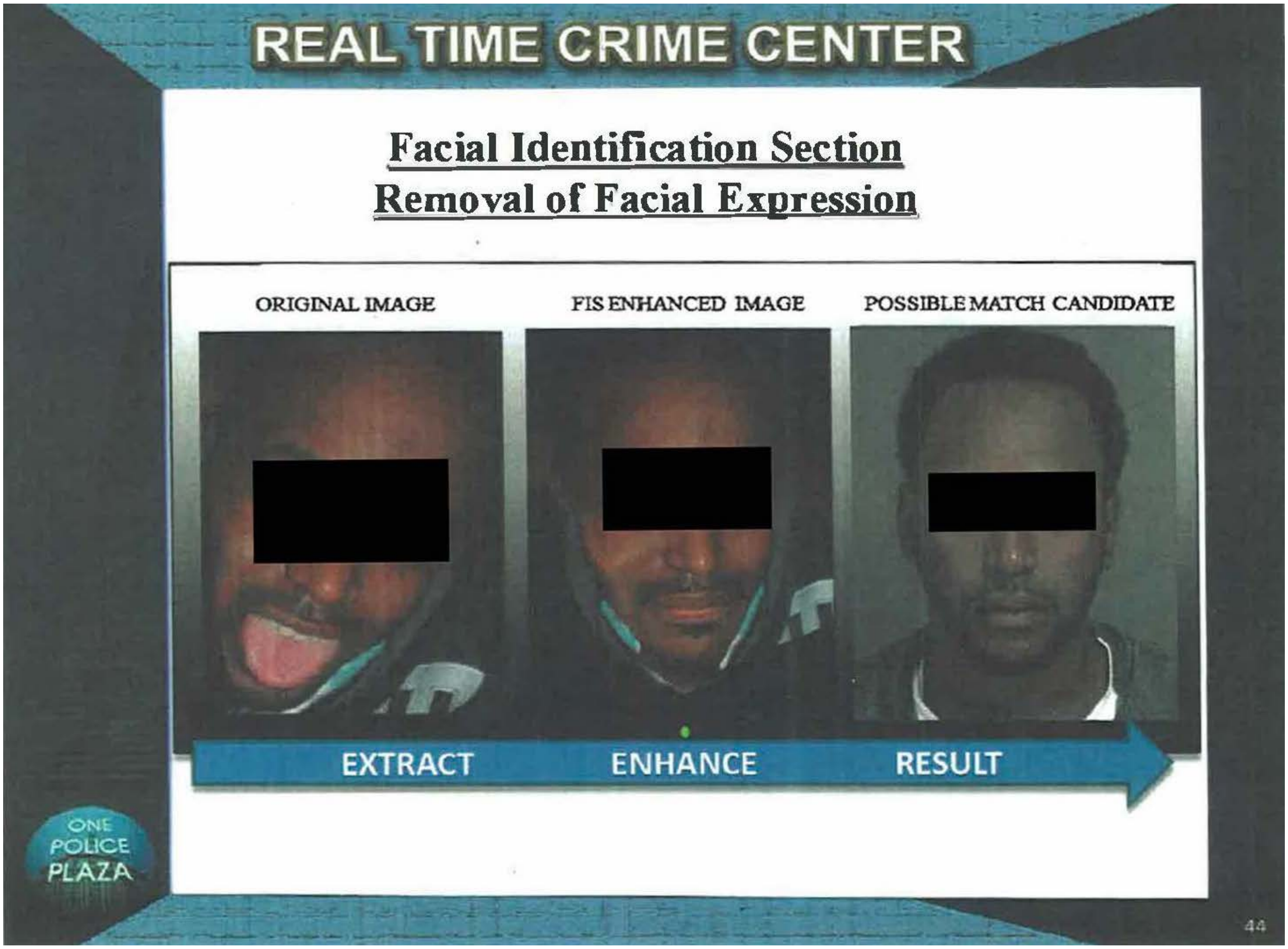
One technique that the NYPD uses involves replacing facial features or expressions in a probe photo with ones that more closely resemble those in mugshots—collected from photos of other people. Presentations and interviews about FIS include the following examples:

- "Removal of Facial Expression"—such as replacing an open mouth with a closed mouth. In one example provided in a NYPD presentation, detectives conducted "...a Google search for Black Male Model" whose lips were then pasted into the probe image over the suspect's mouth.[31]
- "Insertion of Eyes"—the practice of "graphically replacing closed eyes with a set of open eyes in a probe image," generated from a Google search for a pair of open eyes.[32]
- Mirrored effect on a partial face—copying and mirroring a partial face over the Y axis to approximate the missing features, which may include adding "[e]xtra pixels … to create a natural appearance of one single face."[33]
- "Creating a virtual probe"—combining two face photographs of different people whom detectives think look similar to generate a single image to be searched, to locate a match to one of the people

of the combined photograph.[34]

- Using the "Blur effect" on an overexposed or low-quality image—adding pixels to a photo that otherwise doesn't have enough detail "to render a probe that [has] a similar nose, mouth, and brow as that of the suspect in the photo."[35]
- Using the "Clone Stamp Tool" to "create a left cheek and the entire chin area" of a suspect whose face was obscured in the original image.[36]

Another technique that the NYPD and other agencies employ involves using 3D modeling software to complete partial faces and to "normalize" or rotate faces that are turned away from the camera. After generating a 3D model, the software will fill in the missing facial data with an approximation of what it should look like, based on the visible part of what the subject's face looks like as well as the measurements of an "average" face.[37] According to the NYPD, the software creates "a virtual appearance of the suspect looking straight ahead, replicating a pose of a standard mugshot."[38]



REAL TIME CRIME CENTER

Facial Identification Section

Removal of Facial Expression

ORIGINAL IMAGE

[redacted]

FIS ENHANCED IMAGE

[redacted]

POSSIBLE MATCH CANDIDATE

[redacted]

EXTRACT ENHANCE RESULT

Figure 4: A slide from NYPD FIS describing "Removal of Facial Expression" technique. (Source: NYPD.)

These techniques amount to the fabrication of facial identity points: at best an attempt to create information that isn't there in the first place and at worst the introduction of evidence that matches someone other than the person being searched for. During a face recognition search on an edited photo, the algorithm doesn't distinguish between the parts of the face that were in the original evidence—the probe photo—and the parts that were either computer generated or added in by a detective, often from photos of different people unrelated to the crime.[39] This means that the original photo could represent 60 percent of a suspect's face, and yet the algorithm could return a possible match assigned a 95 percent confidence rating, suggesting a high probability of a match to the detective running the search.[40]

If it were discovered that a forensic fingerprint expert was graphically replacing missing or blurry portions of a latent print with computer-generated—or manually drawn—lines, or mirroring over a partial print to complete the finger, it would be a scandal.[41] The revelation could lead to thousands of cases being reviewed, possibly even convictions overturned.[42]

3. RESULTS AS "INVESTIGATIVE LEADS ONLY..."

Most agencies do not yet consider face recognition to be a positive identification. Many law enforcement agencies, the NYPD included, state that the results of a face recognition search are possible matches only and must not be used as positive identification.[43]

In theory, this is a valuable check against possible misidentifications, including those introduced into the system by inputting celebrity comparisons, composite sketches, or other computer-altered photographs that don't accurately represent the person being searched for.

However, in most jurisdictions, officers do not appear to receive clear guidance about what additional evidence is needed to corroborate a possible face recognition match. The NYPD guide states: "Additional investigative steps must be performed in order to establish probable cause to arrest the Subject [sic]" of the face recognition search.[44] But what or how many additional steps are needed, and how independent they must be from the face recognition process, is left undefined.

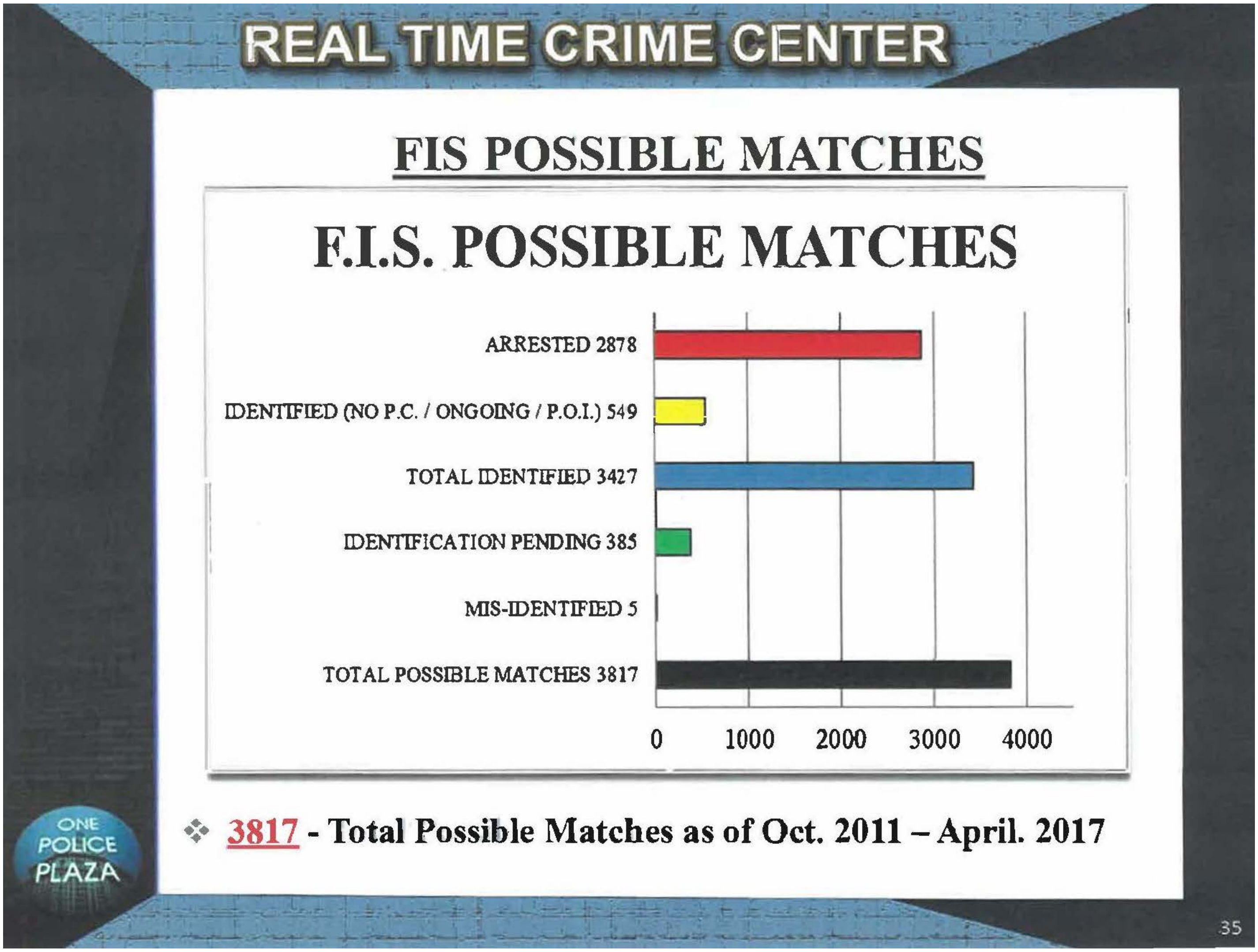
Absent this guidance, the reality is that suspects are being apprehended almost entirely on the basis of face recognition "possible matches." For example:

- In a recent case, NYPD officers apprehended a suspect and placed him in a lineup solely on the basis of a face recognition search result.[45] The ultimate arrest was made on the basis of the resulting witness identification, but the suspect was only in the lineup because of the face recognition process.
- NYPD officers made an arrest after texting a witness a single face recognition "possible match" photograph with accompanying text: "Is this the guy…?" The witness' affirmative response to viewing the single photo and accompanying text, with no live lineup or photo array ever conducted, was the only confirmation of the possible match prior to officers making an arrest.[46]

- Sheriffs in Jacksonville, Florida, who were part of an an undercover drug sale arrested a suspect on the basis of the face recognition search. The only corroboration was the officers' review of the photograph, presented as the "most likely" possible match from the face recognition system.[47]

- A Metro Police Department officer in Washington, D.C., similarly printed out a "possible match" photograph from MPD's face recognition system and presented that single photograph to a witness for confirmation. The resulting arrest warrant application for the person in the photograph used the face recognition match, the witness confirmation, and a social media post about a possible birth date (month and day only) as the only sources of identification evidence.[48]

There are probably many more examples that we don't know about. These represent a fraction of the cases that have used face recognition to assist in making an identification. The NYPD made 2,878 arrests pursuant to face recognition searches in the first 5.5 years of using the technology.[49] Florida law enforcement agencies, including the Jacksonville Sheriff's Office, run on average 8,000 searches per month of the Pinellas County Sheriff's Office face recognition system, which has been in operation since 2001.[50] Many other agencies do not keep close track of how many times their officers run face recognition searches and whether these searches result in an arrest.



❖ 3817 - Total Possible Matches as of Oct. 2011 – April. 2017

Figure 5: In the first 5.5 years of operation, the NYPD's face recognition system led to 2,878 arrests. NYPD Det. Markiewicz estimates that 8,000 cases will have used a face recognition search in 2018 alone. (Source: NYPD.)

Another valuable check against mistaken identification—and unreliable investigative leads—would be to allow defendants access to the inputs and outputs of a face recognition search that resulted in their arrest. But this does not happen. Even though prosecutors are required under federal law to disclose any evidence that may exonerate the accused, defense attorneys are not typically provided with information about "virtual probes," celebrity doppelgängers, or really any information about the role face recognition played in identifying their client.[51] This is a failure of the criminal justice system to protect defendants' due process.[52]

It may be that many of those arrested on the basis of questionable face recognition searches did in fact commit the crime of which they were accused. But the possibility that they didn't—that the face recognition system identified the wrong person—looms large in the absence of additional, independent police investigation and sufficient access to the evidence by the defense. This is risky, and the consequences will be borne by people investigated, arrested, and charged for crimes they didn't commit.

4. CONCLUSION AND RECOMMENDATIONS

There is no easy way to discover just how broad of a trend this represents—and just how many arrests have been made in large part on the basis of celebrity lookalikes, artist sketches, or graphically altered faces submitted to face recognition systems.[53]

But we can anticipate that the problem will get a lot bigger. Police departments across the country are increasingly relying on face recognition systems to assist their investigations. In addition, an official for the Federal Bureau of Investigation (FBI), which runs its own face recognition system, has indicated that the agency plans to do away with the "investigative lead only" limitation altogether. At a conference in 2018, FBI Section Chief for Biometric Services Bill McKinsey said of the FBI: "We're pretty confident we're going to have face [recognition] at positive ID in two to three years."[54]

In setting this goal, the FBI has assumed that the results of face recognition systems will become more accurate as the algorithms improve. But these improvements won't matter much if there are no standards governing what police departments can feed into these systems. In the absence of those rules, we believe that a moratorium on local, state, and federal law enforcement use of face recognition is appropriate and necessary.

The stakes are too high in criminal investigations to rely on unreliable —or wrong—inputs.

Law enforcement agencies that persist in using face recognition in their investigations should at a minimum take steps to reduce the risk of misidentification and mistake on the basis of unreliable evidence. These steps include:

- Stop using celebrity look-alike probe images. Face recognition is generally considered to be a biometric, albeit an imperfect one. Police cannot substitute one person's biometrics for another's, regardless of whatever passing resemblance they may have.
- Stop submitting artist or composite sketches to face recognition systems not expressly designed for this purpose. Sketches are highly unlikely to result in a correct match—and carry a real risk of resulting in a misidentification that a human review of the possible matches cannot correct.
- Establish and follow minimum photo quality standards, such as pixel density and the percent of the face that must be visible in the original photo, and prohibit the practice of pasting other people's facial features into a probe. Any photo not meeting these minimum standards should be discarded —not enhanced through the addition of new identity points like another person's mouth or eyes.
- If edits to probe images are made, carefully document these edits and their results. Retain all versions of the probe image submitted to the face recognition system for production to the defense.
- Require that any subsequent human review of the face recognition possible match be conducted against the original photo, not a photo that has undergone any enhancements, including color and pose correction.
- As is the practice in some police departments, require double-blind confirmation. The face recognition system should produce an investigative lead only if two analysts independently conclude that the same photo is a possible match.
- Provide concrete guidance to investigating officers about what constitutes sufficient corroboration of a possible match generated by a face recognition system before law enforcement action is taken against a suspect. This should include: mandatory photo arrays; a prohibition on informing witnesses that face recognition was used; and a concrete nexus between the suspect and the crime in addition to the identification, such as a shared address.
- Make available to the defense any information about the use of face recognition, including the original probe photo, any edits that were made to that photo prior to search, the resulting candidate

list and the defendant's rank within that list, and the human review that corroborated the possible match.

- Prohibit the use of face recognition as a positive identification under any circumstance.

These recommendations should be considered as minimum requirements, and are made in addition to the broader recommendations the Center on Privacy & Technology made in its 2016 report, *The Perpetual Line-up: Unregulated Police Face Recognition in America* (https://www.perpetuallineup.org/).[55]

As the technology behind these face recognition systems continues to improve, it is natural to assume that the investigative leads become more accurate. Yet without rules governing what can—and cannot—be submitted as a probe photo, this is far from a guarantee. Garbage in will still lead to garbage out.

5. ACKNOWLEDGEMENTS

This report would not be possible without the tireless advocacy of Professor David Vladeck, Stephanie Glaberson, and numerous student lawyers of the Georgetown Law Civil Litigation Clinic, which represents the Center on Privacy & Technology in our public records lawsuit against the New York City Police Department. Only with the assistance of the clinic have we been able to recover thousands of pages of documents regarding use of face recognition technology by the NYPD, even though the agency itself has tried hard to keep its use of this technology hidden from public view.

Critical guidance and close reading were provided by our team of outside reviewers, who will remain anonymous, but who lent us their expertise on New York City policing, criminal litigation, and the technical functioning of face recognition systems. This report would not be possible without the entire team at the Center, who helped in countless ways: Alvaro Bedoya, Laura Moy, Katie Evans, Harrison Rudolph, Jameson Spivack, Gabrielle Rejouis, and Julia Chrusciel. We are also grateful to the Center's research assistants and summer fellows; our copy editor, Joy Metcalf; our design and web development firm, Rootid; and our cover designer, Eve Tyler.

We also acknowledge, with gratitude, the work of our friends and allies at other organizations also striving to shed light on how face recognition technology is used and to prevent powerful police tools from being used in ways that are harmful to individuals and communities. In particular, perhaps no one has done more to address and expose harmful, secret, and unfair uses of police technology than criminal defense attorneys, many of whom continue to provide us with invaluable guidance.

The Center on Privacy & Technology at Georgetown Law is supported by the Ford Foundation, the Open Society Foundations, the MacArthur Foundation, Luminate, the Media Democracy Fund, and Georgetown University Law Center.

1. NYPD, Real Time Crime Center Facial Identification Section (FIS), presentation by Detective Markiewicz (Sept. 17, 2018) (notes on file with author).

2. *Id.*

3. *See, e.g.*, Eric Sofge, *The End of Anonymity*, Popular Science (Jan. 15, 2014), https://www.popsci.com/article/technology/end-anonymity (https://www.popsci.com/article/technology/end-anonymity) (describing the Pennsylvania system as used in Cheltenham Township, Pa.).

4. *See, e.g.*, Washington County Sheriff's Office, *PSWeb Facial Recognition Training Guide,* 47, *available at* https://www.aclunc.org/docs/20180522_ARD.pdf#page=47 (PDF) (https://www.aclunc.org/docs/20180522_ARD.pdf#page=47).

5. NYPD, *Facial Identification Section Case #8: Celebrity Comparison*, Document p. 025428 (https://drive.google.com/drive/folders/1OxzGtFuWBU9PecG2cmpE8QfVwZm9kr22?usp=sharing). The name and image of the New York Knicks player has been redacted in the files provided to the Center by the NYPD.

6. *See* Phoebe Weston, *Who is YOUR celebrity lookalike? Find out with this online AI tool that reveals your famous doppelganger*, Daily Mail (Mar. 30, 2017) https://www.dailymail.co.uk/sciencetech/article-4363640/Who-celebrity-lookalike-online-tool.html (https://www.dailymail.co.uk/sciencetech/article-4363640/Who-celebrity-lookalike-online-tool.html).

7. Hamza Shaban, *A Google app that matches your face to artwork is wildly popular. It's also raising privacy concerns.*, Washington Post (Jan. 17, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/01/16/google-app-that-matches-your-face-to-artwork-is-wildly-popular-its-also-raising-privacy-concerns/ (https://www.washingtonpost.com/news/the-switch/wp/2018/01/16/google-app-that-matches-your-face-to-artwork-is-wildly-popular-its-also-raising-privacy-concerns/).

8. Charles Babbage, *Passages from the Life of a Philosopher* 67 (Longman, Green, Longman, Roberts, & Green ed. 1864).

9. *See* Zhifei Wang et al., *Low-resolution face recognition: a review*, 30 The Visual Computer 359, 359–360 (April 2014), *available at* https://link.springer.com/article/10.1007/s00371-013-0861-x (https://link.springer.com/article/10.1007/s00371-013-0861-x).

10. Patrick Grother et al., National Institute of Standards and Technology, *Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification* 2 (Nov. 2018), https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf (PDF) (https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf) ("The major result of the evaluation is that massive gains in accuracy have been achieved in the last five years (2013–2018).").

11. Stephen Manusci, The Police Composite Sketch 6–7 (Humana Press 2010).

12. Art Selfie, Google Arts & Culture, https://artsandculture.google.com/camera/selfie (https://artsandculture.google.com/camera/selfie) (last accessed Jan. 28, 2019).

13. Maricopa County Sheriff's Office (MCSO), *Counter-Terrorism Information Center Facial Recognition*, Document p. 014951 (https://drive.google.com/drive/folders/0B-MxWJP0ZmePR2xTYzl4ZWZ0Wkk?usp=sharing); MCSO, *Homeland Security & National Facial Recognition Network Briefing Paper* (Oct. 6, 2008), Document p. 014952 (https://drive.google.com/drive/folders/0B-MxWJP0ZmePR2xTYzl4ZWZ0Wkk?usp=sharing); MCSO, MCSO/ACTIC *Facial Recognition Procedures: Image Records Request*, Document p. 014962 (https://drive.google.com/drive/folders/0B-MxWJP0ZmePR2xTYzl4ZWZ0Wkk?usp=sharing).

14. Washington County Sheriff's Office, *PSWeb Facial Recognition Training Guide*, 47, *available at* https://www.aclunc.org/docs/20180522_ARD.pdf#page=47 (PDF) (https://www.aclunc.org/docs/20180522_ARD.pdf#page=47).

15. Nlets, *Privacy Impact Assessment Report for the Utilization of Facial Recognition Technologies to Identify Subjects in the Field* (2011), Document p. 016668 (https://drive.google.com/drive/folders/0B-MxWJP0ZmePSi04Wkd5OG1vanc?usp=sharing).

16. Baltimore Police Dep't, *Governor's Office of Crime Control & Prevention (GOCCP) Fact Sheet: Facial Recognition* (Apr. 2015), Document p. 010954 (https://drive.google.com/drive/folders/0B-MxWJP0ZmePbVh2U2tKcmhaRWs?

usp=sharing); Maryland Dep't of Public Safety & Correctional Services, *GOCCP Fact Sheet: Criminal Justice Dashboard* (Apr. 2015), Document p. 011104 (https://drive.google.com/drive/folders/0B-MxWJP0ZmePZndGQmUtVmNDWEU?usp=sharing); Northern Virginia Regional Information System, *LOB #207: NOVARIS* (2016), Document p. 015231 (https://drive.google.com/drive/folders/0B-MxWJP0ZmePU0MwbXhZY0lickE?usp=sharing); Pinellas County Sheriff's Office, *Interagency Use of Facial Recognition...Does it work?*, 43–52, *available at* https://www.aamva.org/uploadedFiles/MainSite/Content/EventsEducation/Event_Materials/2013/2013_Region_II_Conference/061013_10_30_FR_Complete.pdf (PDF) (https://www.aamva.org/uploadedFiles/MainSite/Content/EventsEducation/Event_Materials/2013/2013_Region_II_Conference/061013_10_30_FR_Complete.pdf).

17. Center for Advancing Retail and Technology, *Cognitec: FaceVACS-VideoScan*, https://www.advancingretail.org/solutions/cognitec (https://www.advancingretail.org/solutions/cognitec). ("Law enforcement professionals can identify individuals in crime scene photos, videos stills and sketches by matching facial images against the agency's mugshot repository"). *See also:* Cognitec, FaceVACS-DBScan LE: Face Recognition Technology for for image and video investigations, and database matching, https://www.cognitec.com/files/layout/downloads/FaceVACS-DBScan-LE-1-1-flyer.pdf (PDF) (https://www.cognitec.com/files/layout/downloads/FaceVACS-DBScan-LE-1-1-flyer.pdf) ("supports investigation of faces in video footage, still images and sketches").

18. Vigilant Solutions, *FaceSearch,* https://www.vigilantsolutions.com/products/facial-recognition/ (https://www.vigilantsolutions.com/products/facial-recognition/)(last viewed May 13, 2019). Vigilant Solutions is now part of Motorola Solutions. *See* Susan Crandall, *Motorola Solutions Acquires VaaS Holdings, Leader in Data and Image Analytics for Vehicle Location*, Vigilant Solutions (Jan. 7, 2019), https://www.vigilantsolutions.com/motorola-solutions-acquires-vaas-international-holdings-leader-data-image-analytics-vehicle-location/ (https://www.vigilantsolutions.com/motorola-solutions-acquires-vaas-international-holdings-leader-data-image-analytics-vehicle-location/). In a 2008 contract to provide a face recognition solution to Utah's Department of Public Safety, Hummingbird Communications also indicated that its solution can "identify individuals from … Police Artist Sketches … or any image from any number or variety of sources." Utah State Analysis and Information Center, *State of Utah Contract with Hummingbird Garden Ranch LLC (*Dec. 22, 2008), Document p. 108705 (https://drive.google.com/drive/folders/0B-MxWJP0ZmePc1QxZGtuNXVaOFU?usp=sharing).

19. Los Angeles County Sheriff's Office, *Facial Recognition & Comparison: Create a Good Source Image*, Document p. 000681 (https://drive.google.com/drive/folders/0B-MxWJP0ZmePOGVuSE1qRFVaM2c?usp=sharing).

20. Anil Jain et al, *Face Recognition: Some Challenges in Forensics*, IEEE Int'l Conference on Automatic Face and Gesture Recognition (Mar. 2011), *available at* https://ieeexplore.ieee.org/document/5771338 (https://ieeexplore.ieee.org/document/5771338).

21. Scott Klum, Hu Han, Anil Jain, & Brendan Klare, *Sketch Based Face Recognition: Forensic vs. Composite Sketches* (2013), *available at* https://openbiometrics.org/publications/klum2013sketch.pdf (PDF) (https://openbiometrics.org/publications/klum2013sketch.pdf) ("In forensic and biometrics scenarios involving facial sketch to mugshot matching, the standard procedure involves law enforcement officers looking through top-N matches (rather than only considering rank-one retrieval rates). In our experiments, N = 200. We also used the performance of a commercial-off-the-shelf face matcher, FaceVACS v8.2 as a baseline. As shown in Fig. 5, FaceVACS achieves rank-200 retrieval rates of 4.1% and 6.7% for forensic and composite sketches, respectively.")

22. *Id.*

23. Patrick Grother & Mei Ngan, *Face Recognition Vendor Test (FRVT): Performance of Face Identification Algorithms, NIST Interagency Report 8009*, 4 (May 26, 2014) https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.8009.pdf (PDF) (https://nvlpubs.nist.gov/nistpubs/ir/2014/NIST.IR.8009.pdf) ("By searching a non-operational set of sketch images against photographs seeded into a population of 640,000 nonmated mugshots, the most accurate algorithms produce the mated photograph only infrequently: The mate is not among the top 50 candidates at the following rates: 73.3% (3M/Cogent), 73.8% (NEC), 78.5% (Toshiba), 80.3% (Morpho), and 81.5% (Neurotechnology).") Note these accuracy

results appear much higher than those in the Michigan State University study, likely because NIST used sketches created by an artist viewing the mugshot, not sketches created based on an eyewitness description of the suspect, which is more akin to real-world scenarios. *Id.* at 39–40 ("the fact that the sketches were prepared by an artist viewing the exemplar photograph probably means that the accuracy measurements here represent a "best case" upper bound on accuracy.").

24. *FIS Presentation* (Sept. 17, 2018) (on file with author).

25. Lance Taylor, Ga. Dep't Driver Serv., Moderation of Interagency Use of Facial Recognition… Does it Work? at the 2013 AAMVA Region II Conference 43–53 (June 10, 2013), https://www.aamva.org/uploadedFiles/MainSite/Content/EventsEducation/Event_Materials/2013/2013_Region_II_Conference/061013_10_30_FR_Complete.pdf (PDF) (https://www.aamva.org/uploadedFiles/MainSite/Content/EventsEducation/Event_Materials/2013/2013_Region_II_Conference/061013_10_30_FR_Complete.pdf).

26. *See* Anil Jain et. al., *Face Recognition: Some Challenges in Forensics*, IEEE Int'l Conference on Automatic Face and Gesture Recognition (Mar. 19, 2011), https://ieeexplore.ieee.org/document/5771338 (https://ieeexplore.ieee.org/document/5771338).

27. *See* Stephen Manusci, The Police Composite Sketch 22–23 (Humana Press 2010). ("It is essential to realize that a composite sketch is a drawing of a victim's or witness's perception of a perpetrator at the time he or she was observed. It is not meant to be an exact portrait of the suspect. Keep the two words "likeness" and "similarity" in mind at all times … Unfortunately, the composite artist does not have an image of the subject in front of him or her while working. The composite artist needs to rely on the verbal description supplied by the witness. Thus, the look of a composite sketch will range from a portrait-type drawing to a caricature-type sketch, unfortunately never achieving either."), 70 ("How the forensic artist applies these witness and victim impressions and presumptions is certainly subjective.")

28. Forensic sketch artists report that eyewitnesses are likely to use analogies, such as a "horse face" or "bug eyes" when describing subjects. *See, e.g.* Manusci, The Police Composite Sketch, at 73, 86.

29. Rodger Rodriguez, *Facial Recognition: Art or Science?*, Vigilant Solutions (Apr. 4, 2016), http://www2.vigilantsolutions.com/facial-recognition-art-or-science-whitepaper (http://www2.vigilantsolutions.com/facial-recognition-art-or-science-whitepaper). Note that Roger Rodriguez is a former detective with the NYPD, credited for helping implement the NYPD's face recognition program.

30. *Id.*

31. *FIS Presentation* (Sept. 17, 2018) (on file with author); Document pp. 020423–24 (https://drive.google.com/drive/folders/1OxzGtFuWBU9PecG2cmpE8QfVwZm9kr22?usp=sharing), 025457 (https://drive.google.com/drive/folders/1OxzGtFuWBU9PecG2cmpE8QfVwZm9kr22?usp=sharing).

32. Michelle Taylor, *The Art of Facial Recognition*, Forensic Mag. (Mar. 13, 2017), https://www.forensicmag.com/article/2017/03/art-facial-recognition (https://www.forensicmag.com/article/2017/03/art-facial-recognition). This was corroborated by Detective Tom Markiewicz in a presentation on NYPD FIS September 17, 2018. Det. Markiewicz provided the example where a photo of a suspect whose eyes were turned to the side returned no possible leads. Replacing them with eyes facing towards the camera yielded a possible match. *FIS Presentation* (Sept. 17, 2018) (on file with author) and Document p. 025463 (https://drive.google.com/drive/folders/1OxzGtFuWBU9PecG2cmpE8QfVwZm9kr22?usp=sharing).

33. *FIS Presentation* (Sept. 17, 2018) (on file with author), NYPD, *Real Time Crime Center FIS Presentation: Partial Face* (Sept. 17, 2018), Document pp. 020421–22 (https://drive.google.com/drive/folders/1OxzGtFuWBU9PecG2cmpE8QfVwZm9kr22?usp=sharing).

34. NYPD, *Real Time Crime Center FIS Presentation: Partial Face* (Sept. 17, 2018, Document pp. 025423, 025466 (https://drive.google.com/drive/folders/1OxzGtFuWBU9PecG2cmpE8QfVwZm9kr22?usp=sharing) ("The goal was to create an image which highlighted the pronounced facial features of the suspect in this image. (Hairline, Forehead, Brows, and Nose). The FIS Investigator utilized the head of [redacted] in the previous case mentioned because of the

similarities to the hairline and forehead. Both photos were combined within the Photoshop software and a Virtual Probe was created.").

35. NYPD, *Real Time Crime Center FIS Presentation: Partial Face* (date unknown), Document pp. 025469–70 (https://drive.google.com/drive/folders/1OxzGtFuWBU9PecG2cmpE8QfVwZm9kr22?usp=sharing).

36. NYPD, *Real Time Crime Center FIS Presentation: Partial Face* (date unknown), Document p. 025458 (https://drive.google.com/drive/folders/1OxzGtFuWBU9PecG2cmpE8QfVwZm9kr22?usp=sharing).

37. For a detailed description of 3D modeling software, see NYPD, *Animetrics User Guide* (May 6, 2017), Document pp. 018287–95 (https://drive.google.com/drive/folders/1OxzGtFuWBU9PecG2cmpE8QfVwZm9kr22?usp=sharing) and NYPD, *DataWorks Plus FACE Plus Case Management User Guide*, Document p. 018235–39 (https://drive.google.com/drive/folders/1OxzGtFuWBU9PecG2cmpE8QfVwZm9kr22?usp=sharing).

38. NYPD, *Sample case 3 of 4 – 3-Dimensional Enhancement* (date unknown), Document p. 025558 (https://drive.google.com/drive/folders/1OxzGtFuWBU9PecG2cmpE8QfVwZm9kr22?usp=sharing).

39. *See, e.g.* Felix Juefei-Xu et al., *A Preliminary Investigation on the Sensitivity of COTS Face Recognition Systems to Forensic Analyst-style Face Processing for Occlusions*, IEEE Conf. on Computer Vision and Pattern Recognition Workshop 25, 31 (2015), http://openaccess.thecvf.com/content_cvpr_workshops_2015/W02/papers/Juefei-Xu_A_Preliminary_Investigation_2015_CVPR_paper.pdf (PDF) (http://openaccess.thecvf.com/content_cvpr_workshops_2015/W02/papers/Juefei-Xu_A_Preliminary_Investigation_2015_CVPR_paper.pdf). (Analysis of the results on edited faces "...questions the credibility of the FRS since the swapped in part contains biometric information of an other subject. It is questionable and surprising that the FRS uses some other biometric information to its benefit.").

40. Not all face recognition systems present the confidence scores of the photos in the candidate list; and of those that do, some are presented as a percentage and some are on a logarithmic or other scale. Percentages are being used here for illustrative purposes.

41. Latent fingerprints, fingerprints left unintentionally on surfaces and lifted for investigative purposes, may be subject to "preprocessing," editing. However, the goal of this editing is to "improve the retrievable information in a latent image while avoiding any edits that alter critical aspects of this [biometric] information." Paul Lee et al., *Forensic Latent Fingerprint Preprocessing Assessment, NISTIR 8215*, NIST, 5 (June 2018), https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8215.pdf (PDF) (https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8215.pdf). Improper or overuse of editing tools leads to "accidentally darkened valleys that blend together with nearby ridges, or adding false minutiae or obscuring potentially usable minutiae." *Id.*

42. For a discussion of the potential consequences of misconduct or error by fingerprint examiners, *see* Tom Jackman, *Orlando Fingerprint Examiner Suspended, 2,600 cases possibly affected in latest police lab scandal*, Washington Post, Feb. 27, 2017, https://www.washingtonpost.com/news/true-crime/wp/2017/02/27/orlando-fingerprint-examiner-suspended-2600-cases-possibly-affected-in-latest-police-lab-scandal/ (https://www.washingtonpost.com/news/true-crime/wp/2017/02/27/orlando-fingerprint-examiner-suspended-2600-cases-possibly-affected-in-latest-police-lab-scandal/); Simon A. Cole, *Scandal, Fraud, and the Reform of Forensic Science: The Case of Fingerprint Analysis*, Cole-Monteleone (Proof), Jan. 21, 2017, available at https://wvlawreview.wvu.edu/files/d/94befc60-12bc-47d5-9e72-c8249a566415/cole-monteleone-post-page-proof.pdf (PDF) (https://wvlawreview.wvu.edu/files/d/94befc60-12bc-47d5-9e72-c8249a566415/cole-monteleone-post-page-proof.pdf).

43. NYPD, *Real Time Crime Center Facial Identification Section (FIS) Notifications, Chief of Detectives Memo No. 3* (Mar. 27 2012), Document pp. 017349–52 (https://drive.google.com/drive/folders/1OxzGtFuWBU9PecG2cmpE8QfVwZm9kr22?usp=sharing). ("Real Time Crime Center Facial Identification Section (FIS) analyst determines that Subject is POSSIBLY the suspect whose image is depicted in the video and / or photograph regarding a crime. A FIS Possible Match does NOT constitute a positive identification and does NOT establish probable cause to arrest the Subject. Additional investigative steps MUST be performed in order to establish probable cause to arrest the Subject." (emphasis in original)).

44. NYPD, *Real Time Crime Center Facial Identification Section (FIS) Notifications, Chief of Detectives Memo No. 3* (Mar. 27, 2012), Document pp. 017349–52 (https://drive.google.com/drive/folders/1OxzGtFuWBU9PecG2cmpE8QfVwZm9kr22?usp=sharing).

45. Specifics withheld given the ongoing nature of this case.

46. Notice of Motion to Suppress Identification Testimony filed before the Supreme Court of the State of New York, Index number withheld, on file with author. Case specifics are not provided given the ongoing nature of the case.

47. Willie Allen Lynch v. State of Florida, 1D16-3290.

48. Superior Court of the District of Columbia Criminal Division, Affidavit in Support of an Arrest Warrant, on file with author. Specifics withheld given the ongoing nature of the case.

49. NYPD, *Real Time Crime Center, FIS Possible Matches as of Oct. 2011–April 2017*, Document no. 018587 (https://drive.google.com/drive/folders/1OxzGtFuWBU9PecG2cmpE8QfVwZm9kr22?usp=sharing) (2878 arrested, 549 additionally identified, 3427 total identified, 385 identification pending, 5 mis-identified, 3817 total possible matches).

50. Pinellas County Sheriff's Office, *Florida's Facial Recognition Network, FACES Training* (2015), Document p. 014396 (https://drive.google.com/drive/folders/0B-MxWJP0ZmePQ2kyMm1LVFVnOTg?usp=sharing).

51. Interviews with public defenders in New York, Washington, D.C, San Francisco, Orlando, Pinellas County, and Baltimore (on file with author). *See generally* Brady v. Maryland, 373 U.S. 83 (1963). *See* Clare Garvie, Alvaro Bedoya & Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America* (Oct. 18, 2016), https://www.perpetuallineup.org/findings/transparency-accountability (https://www.perpetuallineup.org/findings/transparency-accountability) (discussing the fact that in the 15 years the Pinellas County Sheriff's Office system has been using face recognition technology, the Public Defenders Office has never received face recognition information as part of *Brady* disclosure).

52. *See* Lynch v. Florida Amici Curiae brief of American Civil Liberties Union, Electronic Frontier Foundation, Georgetown Law's Center on Privacy & Technology, and Innocence Project in support of petitioner, No. SC2019-0298 (2019), *available at* https://efactssc-public.flcourts.org/casedocuments/2019/298/2019-298_notice_86166_notice2dappendix2fattachment20to20notice.pdf (PDF) (https://efactssc-public.flcourts.org/casedocuments/2019/298/2019-298_notice_86166_notice2dappendix2fattachment20to20notice.pdf).

53. Based on records provided to us from the NYPD, we have an approximate number of the arrests made that involved some face recognition search total, but this is not disaggregated by photo editing or probe photo format. Between October 2011 and April 2017, NYPD arrested 2,878 individuals based in part on a face recognition possible match, and ran a total of 3,817 searches. *See* NYPD, *Real Time Crime Center FIS Possible Matches* (Feb. 9, 2018), Document p. 018587 (https://drive.google.com/drive/folders/1OxzGtFuWBU9PecG2cmpE8QfVwZm9kr22?usp=sharing). In September 2018, FIS Detective Markiewicz anticipated a total of 8,000 NYPD cases to have involved a face recognition search by the end of the year. *FIS Presentation* (Sept. 17, 2018) (on file with author).

54. IJIS Institute National Symposium (Feb. 7, 2018) (on file with author).

55. Clare Garvie, Alvaro Bedoya & Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America* (Oct. 18, 2016), https://www.perpetuallineup.org/recommendations (https://www.perpetuallineup.org/recommendations).

Site by Rootid (https://rootid.com)